CRYPTOGRAPHIC TRAP DOOR WITH TIMED LOCK AND CONTROLLED ESCROW

ABSTRACT OF THE DISCLOSURE

In a secure communication employing keys which require updating, all parties to the communication update their keys according to a clock at a suitable agreed-upon interval, and the keys are updated once each interval via a one-way function. The key to be used for a communication is the one that is current when the communication is established. In order to address clock-slip and slight timing differences across a communication channel, each party to a paired communication send a current interval index of their key to the other party. The remote index, i.e., the interval index which is remote to the receiving party, is compared against the local interval index, and the latter of the two interval indexes is used as the basis for generating the key. The party with the earlier index must therefore update the key iteratively until its index is concurrent with the later index. In addition, a public-key, private-key pair is generated for the purpose of supporting key updating. To this end, an escrow agent is provided to generate the public-key and private key-pair and to distribute the public key to all parties wishing to engage in key updating, while securing the private key.